ABSTRACT OF THE DISCLOSURE

A real-time approach to detecting aberrant modes of system behavior induced by abnormal and unauthorized system activities indicative of abnormal activity of a software system is based on behavioral information obtained from a suitably instrumented computer program as it is executing. The theoretical foundation is founded on a study of the internal behavior of the software system. As a software system is executing, it expresses a set of its many functionalities as sequential events. Each of these functionalities has a characteristic set of modules that is executed to implement the functionality. These module sets execute with defined and measurable execution profiles among the program modules and within the execution paths of the individual modules, which change as the executed functionalities change. Over time, the normal behavior of the system will be defined by the boundary of the profiles. Abnormal activity of the system will result in behavior that is outside the normal activity of the system and thus result in a perturbation of the system in a manner outside the scope of the normal profiles. Such anomalies are detected by analysis and comparison of the profiles generated from an instrumented software system against a set of nominal execution profiles. Moreover, a method for reducing the amount of information necessary to understand the functional characteristics of an executing software system identifies the common sources of variation among the program instrumentation point frequencies and builds execution profiles based on a reduced set of virtual execution domains.